Fall 2010
Volume 2, Issue 1

Published quarterly by DoD PKE

# *The* PKE *Quarterly Post*

## Enforcing Certificate Assurance Levels for Secure Interoperability

By Julia Ott

With the DoD's increasing emphasis on the need for secure information sharing and interoperability with mission partners, we are seeing PKI policy being developed and expanded to support information sharing objectives while maintaining the strength of the Department's security posture. The DoD Chief Information Officer (CIO) Memorandum "Approval of External Public Key Infrastructures" dated July 22, 2008 approved partner PKIs and credentials which meet specific requirements for use with DoD systems. DoD Instruction (DoDI) 8520.02 regarding Public Key Infrastructure (PKI) and Public Key Enabling (PKE), which will supersede DoDI 8520.2 and is currently in SD106 coordination, codifies and expands upon the partner interoperability requirements established by the July 2008 DoD CIO memo. The DoD External Interoperability Plan provides further detail on the process partners must follow to receive DoD approval for use, and DoDI 8520.cc regarding Identity Authentication for Information Systems (also in SD106 coordination at time of press) defines credential type and assurance level requirements for DoD systems based on hosting environment and data sensitivity.

*continued on page 3*

### In This Issue



### In Every Issue

## Ask the Expert

By Nicole Baker

**Question:** How do we obtain the latest version of Tumbleweed or CoreStreet?

**Answer:** There are two OCSP plug-in software packages approved for use within the DoD: Tumbleweed and Corestreet. This software is only available through your organization due to licensing agreements. Both Tumbleweed and CoreStreet have been purchased by other companies. Axway has purchased Tumbleweed and ActivIdentity has purchased CoreStreet. Organizations may begin to see these new company names associated with the OCSP software products. The DoD PKE Engineering website has a comprehensive list of organizational contacts located at http://iase.disa.mil/pki-pke/contact.html.

**Question:** I would like to stand up an organizational (local) OCSP responder. We have been instructed to use RCVS proof sets. What are proof sets and where can we obtain them?

**Answer:** Proof sets are files containing pre-signed responses for all certificates in the DoD. Proof sets are required when using this type of responder. Proof sets can be obtained by pointing your local OCSP responder to the following URLs:

### Corestreet Proof Sets

These are available on port 80 and 6391:

http://sa.disa.mil:6391/proofs/ = CONUS sites
http://214.24.177.146:6391/proofs/ = EUCOM PS
http://207.133.227.112:6391/proofs/ = PACOM PS

### Tumbleweed Proof Sets

http://sa.disa.mil:6132/proofs/ = CONUS sites
http://214.24.177.146:6132/proofs/ = EUCOM PS
http://207.133.227.112:6132/proofs/ = PACOM PS

*continued on page 3*

# Notes from DoD PKE

By Allison Scogin, DoD PKE Team Lead

It's been a very busy and exciting fall for the DoD PKE team! We were sad to bid farewell to Cammie Webster in August as she moved on from DISA to a position in the private sector, but are thrilled to welcome Phil Scheffler to the team. Phil is an Information Assurance Scholarship Program (IASP) intern who joined DISA after completing his masters in Computer Science at Boston University this past May. He joined the PKE team in August and has already proven himself an invaluable asset to the program. He is looking forward to meeting members of the community and working to solve some of the challenges they face.

In the first half of September, the DoD PKE team provided on-site engineering support to the United States European Command (EUCOM)-sponsored Combined Endeavor 2010 exercise conducted in Germany. Support included the development and deployment of a Coalition PKI Root and Subordinate Certification Authority (CA) along with a Microsoft Enterprise CA to support IPSec Simple Certificate Enrollment Protocol (SCEP) auto-enrollment. The PKE team provided PK-enabling support to the various nations at the exercise during the pre-test and testing phases. This PK-enabling support ranged from certificate issuance and validation to PK-enablement of specific products such as Microsoft IIS, Apache web server, email clients and Cisco routers.

As the SIPR hardware token operational assessment progresses, the PKE team has been working to equip the community with the knowledge they need to enable their systems to use the new tokens. The team has been performing product testing, interfacing with vendors, and developing guidance to support a smooth production roll-out. A full list of the SIPRNet reference guides available at time of press can be found in the Latest Document Releases section of this newsletter.

The PKE team is also supporting the DoD OCIO in their coordination of the DoD SHA-256 evaluation currently underway. The purpose of the evaluation is to identify deployed systems across the DoD that will be affected by the federal government's migration to the usage of SHA-256, then develop mitigation strategies and timelines to ensure continuity of operations during the migration. The PKE team is serving as the technical point of contact for the evaluation process, and will be providing both structured and ad hoc testing guidance for the CC/S/As as they work to evaluate their systems. Visit our SHA-256 coordination page at http://iase.disa.mil/pki-pke/sha256 to get the latest SHA-256 evaluation materials.

# Missing Encryption Certificates in Outlook 2007

By Dan Jeffers

The DoD PKE team received reports this summer from Outlook 2007 users who were unable to save sender encryption certificates into their Outlook Contacts, making sending encrypted emails unusually cumbersome. The PKE team has determined that the issue was introduced with Microsoft Security Patch KB980376.

### Microsoft Resolution

Microsoft is currently working on a patch to resolve the issue, which has not been finalized but is available here: http://support.microsoft.com/kb/2276479. If you are not severely affected by this problem, we recommend that you wait for the next software update that contains this hot fix. Alternatively, at Administrator discretion, it is possible to remove the security patch by following the steps listed here: http://support.microsoft.com/kb/980376. If you are experiencing this issue and prefer not to apply the hot fix or remove the security patch that introduced the issue, there are a couple of alternative approaches to addressing the issue.

### Alternative Method #1

DoD users can look up and find each other in either one of DoD's enterprise directory services.

- Joint Enterprise Directory Services (JEDS): https://jeds.gds.disa.mil
- Global Directory Service (GDS) 411: https://dod411.gds.disa.mil

### Alternative Method #2

For DoD relying parties who use ActivIdentity middleware, there is an option in the *ActivIdentity Advanced Configuration Manager* under *Outlook Enhancements* called *"Automatically add sender's certificate to Outlook contacts"* which can be set to "Yes."

## Enforcing Certificate Assurance Levels for Secure Interoperability – *continued*

| Current Requirements for Acceptance of Partner PKI Credentials* (as established by DoD CIO Memo "Approval of External Public Key Infrastructures"**) | |
|---|---|
| Federal Agency PKIs | Cross-certified with the Federal Bridge at Medium Hardware or High Assurance<br>OR<br>Operated by a Shared Service Provider (SSP) under Common Policy and asserts id-fpki-common-hardware or id-fpki-common-authentication policy OID |
| Non-Federal Agency PKIs | Cross-certified with the Federal Bridge at Medium Hardware Assurance either directly or via membership in another cross-certified PKI bridge (e.g. CertiPath)<br>AND<br>Have a DoD sponsor who establishes a business or mission need, with a Memorandum of Agreement (MoA) in place |

*All partner PKI approvals are also contingent upon successful completion of interoperability testing by the Joint Interoperability Test Command (JITC). A current list of approved partner PKIs is available on the DKO External Interoperability site at https://www.us.army.mil/suite/page/571419.
** The memo also establishes requirements for acceptance of Foreign, Allied, and Coalition Partner PKI credentials which are omitted here due to their being beyond the scope of assurance level filtering.

As policy continues to facilitate and emphasize interoperability, and initiatives to enable DoD systems to accept partner-issued credentials ramp up, the focus is often on which PKIs are and are not approved for use, while the assurance level stipulations get lost in the shuffle. This approach leaves a gaping hole in the security of the infrastructure, since the assurance level dictates the level of confidence we can have in the identity of the subject. The difference between credentials of Rudimentary and Medium assurance levels, for example, translates to the difference between a user who simply provided a functioning email address to obtain a credential (Rudimentary assurance) and one who provided two forms of official government-issued ID in person to a trusted agent (Medium assurance).

So to have confidence in the identity of the authenticating user, it is critical to check and enforce the certificate's assurance level in accordance with DoD policy. But how do we do that?

Assurance levels are technically represented as certificate policy object identifiers (OIDs), which are strings of numbers defined in the issuing organization's certificate policy as corresponding to specific assurance levels for that organization. The policy OID corresponding to a particular certificate's assurance level is included in the certificate's Certificate Policies extension, so that is where we need to look to determine if a certificate's assurance level is acceptable for DoD use. This process is called OID filtering.

**The good news:** If your implementation has the capability to do dynamic path building and process cross-certificates, you can trust the DoD Interoperability Root and the cross-certificates that are in place between the DoD Interoperability Root, the Federal Bridge, and its other members will take care of the OID filtering for you through policy mappings contained within the cross-certificates.

**The bad news:** If your system requires you to directly trust each Certificate Authority (CA) in the certificate's trust chain, things are a bit more complex. For each external organization's PKI that you are trusting, you need to identify the OIDs that map to Federal Bridge Medium Hardware or High assurance levels and put mechanisms in place to ensure that only certificates containing those OIDs or approved Common Policy OIDs are accepted for authentication to your system. Since very few COTS or GOTS systems provide this configuration capability out of the box, a third-party plug-in or custom code is often necessary.

To help with interoperability implementations, the DoD PKE team maintains a Partner Certificate Map on the DoD External Interoperability site (https://www.us.army.mil/suite/page/571419) that contains OID mappings to Federal Bridge assurance levels for currently approved PKIs, as well as other information often needed to configure a system with a direct trust model for interoperability with approved partners. The PKE team also publishes Webcullis (http://pkif.sourceforge.net/webcullis.html), a plug-in for IIS and Apache that provides OID enforcement capabilities.

In addition, the DoD PKE team is working to compile a library of code samples from DoD groups that have written custom implementations for COTS or GOTS products to provide OID filtering capabilities. If you have an OID filtering code sample that you would like to share, please email pke_support@disa.mil with the relevant code, product and installation instructions. All submissions will be reviewed prior to publication to the library.

## Ask the Expert - *continued*

**Question:** I am doing some internal testing and I would like to use test certificates. Where can I obtain these?

**Answer:** Test certificates can be obtained through JITC. Information can be found on the JITC website: http://jitc.fhu.disa.mil/pki/pki_lab/obtaining_jitc_issued_test_certificates.html

The JITC root certificates will need to be installed in order to form a trust chain between the test certificate and the JITC root CA. InstallRoot for JITC certificates is locted on the DoD PKE IASE website: https://powhatan.iiie.disa.mil/pki-pke/function_pages/most_requested.html. InstallRoot J installs all of the DoD JITC root and intermediate test CA certificates. JITC root certificates are to be installedon testing computers, not live assets. JITC CRLs are available at: https://crl.gds.nit.disa.mil/. JITC RCVS is available at: http://ocsp.nsn0.rcvs.nit.disa.mil

## RA/LRA/KRA Corner

### KRA 20-Character Passwords

On July 12, 2010 the DoD PKI program completed implementation of a new Key Recovery Authority (KRA) password scheme on the key escrow servers and Automated Key Recovery Agent (ARA) systems. At this point in time, all KRAs should be utilizing their new 20-character passwords to recover keys on the key escrow servers. The new key escrow scheme does not alter the ARA interface, nor does it require subscribers to change the way they use the ARA system.

A DISA designated trusted agent Ngoc Kolbenschlag has sent KRAs their new 20-character passwords in two separate encrypted email messages, along with instructions on combining the two parts of the password. To obtain a copy of the instructions, please contact the he PKE help desk Support Team at PKE_Support@disa.mil.

### 2048-Bit Server Certificate Keys

As of July 2010, DoD requires all issued DoD server certificates to have key lengths of 2048 bits in order to stay ahead of threat vectors. Certificates with the enhanced security of 2048-bit keys are now available and show no noticeable impact in performance or installation. Unless there is a compelling reason to use 1024-bit keys, 2048-bit keys for server certificates should start to be implemented immediately. Key generation instructions have been modified to incorporate this change.

*continued on page 5*

# Wireless Update

By Ross Schwalm

This article covers two topics affecting DoD BlackBerry users: issues sending encrypted emails and a flaw in handling the Robust Certificate Validation Service (RCVS) transition to the Delegated Trust Model (DTM).

### Issues Sending Encrypted Emails

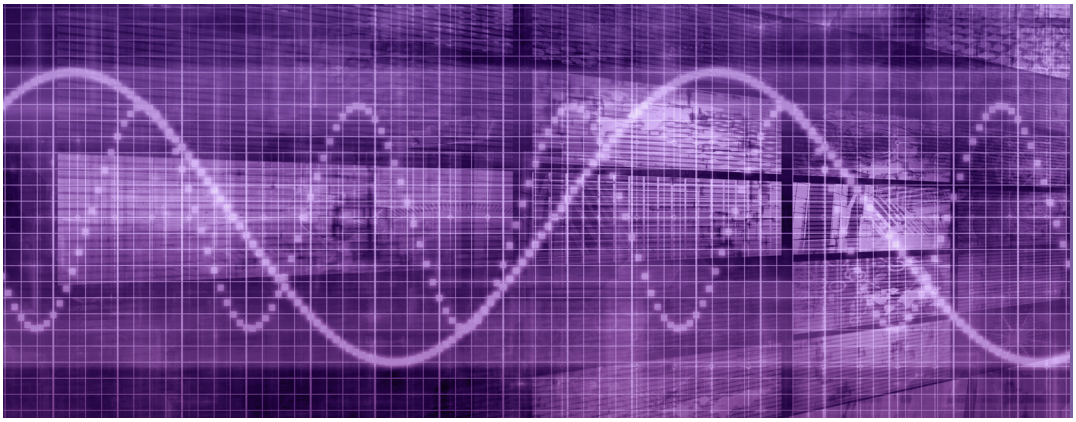
BlackBerry users expect sending an encrypted email to be very similar to the Desktop experience. In many instances it is, but there is one distinct difference, public certificates are stored within the contact on the desktop, while certificates and contacts are stored separately on the BlackBerry. Even though desktop email client contacts can be synced with the BlackBerry address book, the certificates associated with those contacts are not synced. This is usually not a problem because a properly configured BlackBerry Enterprise Server will seamlessly fetch the recipient's public certificate, in most cases. It is not seamless when the email address of the recipient is not known or is different from the email address in the recipient's public certificate. When the email address is properly listed in the BlackBerry address book, the certificate is automatically fetched from DoD411. Without the correct email address, the sender must search DoD411 by recipient first and last name. A worse case occurs when the recipient's email address doesn't match their certificates email address (BlackBerry is unable to fetch or locate the correct certificate in its keystore). To work around this issue, the user must go to Options->Security Options->Certificates and look in the "others" container (displayed in the upper right hand corner) for the recipient's certificate, press the BlackBerry button, and then Associate Addresses. By adding the recipient's email address (which differs from their certificates email address) the process of sending an encrypted email becomes seamless again.

### "The OCSP Responder's Certificate Chain Has Expired or is Not Yet Valid"

Have you received the above message on your BlackBerry? Don't worry, it's not your fault. After the RCVS migration to DTM, there is no longer only one self-signed Online Certificate Service Protocol (OCSP) responder certificate that is valid for three years and included in the BlackBerry InstallRoot package. Each OCSP responder is issued one certificate for every DoD Certificate Authority and this certificate is renewed every 45 days. Renewed OCSP responder certificates are included with certification validation responses similar to a signed email. BlackBerry users have probably been prompted to enter their keystore password for an OCSP responder certificate. The flaw (that has been reported to RIM) occurs in the way a BlackBerry handles certificate renewals for existing certificates in its keystore. At this time there is only a manual work-around for users to search the "others" container in their keystore (location described above) for one or more of these certificates: DoD OCSP NIPRNET 1T 1, DoD OCSP NIPRNET 2T 1, DoD OCSP NIPRNET 5T 1, DoD OCSP NIPRNET 6T 1. One or all of them have been renewed, therefore the user must manually delete them and the issue will disappear, until the next renewal.

# InstallRoot Overview

By Linda Devlin



### Purpose of InstallRoot

InstallRoot is a utility used to manage DoD-authorized trusted Root Certification Authorities (CA) and Intermediate CAs on servers and workstations. InstallRoot comes packaged with the DoD Root and all Intermediate CA certificates.

### Who Needs InstallRoot?

Administrators use InstallRoot to install DoD CA certificates on servers used to authenticate clients. Users utilize InstallRoot to install DoD CA certificates on their workstations, so they can authenticate DoD servers utilizing SSL or TLS. Users needing to send and receive secure email on DoD systems use InstallRoot so they can sign and encrypt/decrypt secure email. The DoD CA certificates that InstallRoot adds to the system's trust store are the basis for the trust relationship that must exist between DoD servers and connecting clients, or any other DoD application that uses certificates for digital signature or authentication.

### Graphical User Interface (GUI) vs. Command Line Interface

InstallRoot is available with a GUI that provides the user the ability to select a specific trust store where the certificates will be inserted or deleted. The GUI version also allows the user to select the types of certificates that will be installed and provides two modes of operation: standard and advanced. The standard mode is for novice users just needing to install all certificates of a certain type to the selected trust store. The advanced mode provides more granular control over individual certificates in each trust store, allowing the user to list, insert, or delete specific certificates.

InstallRoot can also be run via a command line interface, where the user specifies options that control the actions that InstallRoot will perform. The command line interface provides the same functionality as the GUI for inserting, listing, and deleting certificates from a system trust store.

### Types of Certificates Installed

The following types of certificates are packaged with InstallRoot:

1. DoD NIPRNET certificates, for systems using the operational DoD PKI (packaged with the "A" command line executable)

2. JITC (Joint Interoperability Test Command) and O&M (Operations and Maintenance) certificates, used on Non-Operational or test systems only (packaged with the "J" command line executable)

3. ECA (External Certificate Authority) certificates, used on systems that need to trust an ECA (packaged with the "E" command line executable)

4. DoD SIPRNET certificates, used only on systems connected to the SIPRNET (packaged with the "S" command line executable)

In the GUI interface, the user selects which of the four types of certificates they wish to add to the system trust store. The command line interface of InstallRoot is available in different versions, according to the type of certificates that need to be installed (as indicated in the above list).

### Trust Stores

In the GUI interface of InstallRoot, the user can choose whether to manage certificates in either the Windows/Internet Explorer system trust store (the default trust store) or the Firefox/Mozilla/Netscape system trust stores. Each user of the workstation has his own Firefox/Mozilla/Netscape trust store, and InstallRoot provides a list of these user trust stores, from which the user can select which trust store to manage.

In the command line interface, the Windows/Internet Explorer trust store is the only system trust store that can be modified.

## DoD LRA/RA and KRA Training

The DoD training schedule for Local Registration Authorities (LRAs), Registration Authorities (RAs) and Key Recovery Agents (KRA) is now posted on the DOD PKE Website. For dates and more details, go to: http://iase.disa.mil/pki-pke/index.html

## Help Desk & Contact Information

To contact your Local Help Desk or organization's Registration Authority (RA), please visit http://iase.disa.mil/pki-pke/contact.html

## In the Pipeline

### Developing Support for New Mobile Devices

For the DoD workforce to be truly mobile, it must have secure on-demand access to NIPRNET services beyond simply email. As the capabilities of emerging mobile platforms such as iOS for iPhone/iPad, Android, Windows Phone 7, and BlackBerry PlayBook QNX OS continue to mature, the demand for support of compatible devices within the DoD grows. Benefits of providing support for mobile devices include increased workforce productivity and improved disaster recovery planning and coordination capabilities.

For these devices to be successfully integrated into the DoD operational environment, enabling identity management capabilities compatible with the existing infrastructure–such as usage of PKI credentials for authentication, digital signature and encryption–is crucial.

*continued on page 6*

## In the Pipeline - *continued*

To that end, the DoD PKE team has stood up a PKE Mobile lab and is currently working to evaluate capabilities and develop guidance for iOS as well as BlackBerry. The team is working closely with vendors to improve mobile PKI capabilities, providing testing feedback and information regarding DoD PKI requirements. The team is also supporting Security Technical Information Guides (STIG) development efforts for both mobile operating systems. Within the next year, the team plans to perform similar work for other popular mobile platforms to enable community members to stay connected, informed, and productive on-the-go.

## About DoD PKE

The DoD Public Key Enabling (PKE) Team is chartered with helping DoD customers leverage existing and emerging PKI capabilities for increased productivity and an improved Information Assurance posture. We provide engineering consultations, develop enterprise solutions, create collaboration environments, and work to make commercial products interoperate with the DoD PKI.

We are committed to increasing the security posture of the DoD by providing a seamless security environment supporting Identity Management efforts with the overarching goal of defending and protecting the United States of America.

***DoD PKE is the Key to operationalizing PKI.***

Visit us on DKO—
http://iase.disa.mil/pki-pke

Send your questions and feedback to—
PKE_Support@disa.mil

# DoD PKI Test Certificates

By Richelle Taylor-Jones

The DoD PKI program provides identity credentials for several different populations within DoD for different purposes. Most of the production infrastructures that provide these credentials have companion test infrastructures for use by DoD's test and development communities. Below is a list of the available DoD PKI test materials and recommended usages:

| # | Test Material | Target Development | Typical Turnaround |
|---|---|---|---|
| A | **DoD PKI Test Software Certificates**<br>• **Target population:** DoD personnel or affiliates who do not utilize hardware tokens or CACs<br>• **Description:** DoD PKI test software certificates that are distributed electronically as PKCS#12 files<br>• **DoD Lead:** DISA<br>• **Location:** Instructions on requesting software certificates can be found at http://jitc.fhu.disa.mil/pki/pki_lab/obtaining_jitc_issued_test_certificates.html | • Web-based applications, portals, and/or websites with browser-based user interfaces (UIs)<br>• Applications that secure cryptographic services from Microsoft Cryptographic Application Interface (CAPI) or CAPI: Next Generation (CNG) | 1-2 business days |
| B | **DoD Test Alternate Tokens**<br>• **Target population:** Non-CAC eligible populations who require access to UNCLASSIFED networked DoD accounts (e.g., selected volunteers or non-US persons)<br>• **Description:** DoD PKI test certificates that come on hardware (i.e., smart cards) procured and managed by the DoD Components. These cards do not contain barcode or contactless technologies<br>• **DoD Lead:** Individual DoD Components<br>• **Location:** This material may be available for selected development/test populations as decided by the PKI Leads for each individual DoD Component. Please contact your Component's PKI Lead below for details:<br>– USAF, AFPKI.Helpdesk@lackland.af.mil<br>– USN, itac@infosec.navy.mil<br>– USMC, james.mcdonald.ctr@mcnosc.usmc.mil<br>– USA, iacacpki.helpdesk@us.army.mil<br>– WHS, whsra@whs.mil | • Applications/devices that service non-CAC eligible personnel<br>• Applications/devices that have knowledge of and technical interfaces to smart cards and/or external tokens and need services directly from them<br>• Application/devices that need services from alternate tokens and process cryptography from tokens on their own, without leveraging web browsers or Microsoft cryptographic capabilities | Varies by DoD Component |
| C | **DoD Test Common Access Card**<br>• **Target population:** DoD military, civilian, and selected contract support personnel<br>• **Description:** DoD test credentials that contain hardware DoD PKI certificates, DoD CAC Data model including JDM applets, FIPS 800-73 interfaces, contactless technology, magnetic stripe, two-dimensional barcode (PDF417), linear barcode (Barcode 39), and conform with FIPS 201<br>• **DoD Lead:** DMDC<br>• **Location:** Test CAC request forms are processed through the DoD Components' test card approval agents. Submissions and inquiries can be made directly to your DoD Component PKI lead or via cacsupport@osd.pentagon.mil. | • Applications/devices that have knowledge of and technical card edge interfaces to smart cards and/or external tokens and need services directly from the CAC<br>• Applications/devices that need services from the CAC and process cryptography from tokens on their own, i.e., without leveraging web browsers or Microsoft cryptographic capabilities | Approximately 25-30 business days |

## Latest Tool Releases

These PKI tools are freely available via SourceForge at http://pkif.sourceforge.net

- **CAPI Logger** CAPI Loger is a diagnostic tool used to collect information about a system's usage of several PKI-related CAPI functions for testing and troubleshooting.

- **PKI** PlugPKI Plug is a revocation status provider for Microsoft CAPI that aims to improve performance and usability of CAPI in cross-certified environments by influencing CAPI path processing to favor shorter certification paths.

- **Cross Certificate Pair Tool** The Cross Certificate Pair Tool is a GUI-based tool that enables easy parsing and creation of cross-certificate pair objects.

- **Cross Certificate Pair Command Line Tool** The Cross Certificate Pair Command Line Tool is a command line version of the Cross Certificate Pair Tool.

## Latest Document Releases

The following documents have been added to or updated on the DoD PKE Knowledge Base at http://iase.disa.mil/pki-pke

- Public Key Enabling Microsoft Internet Information Service (IIS) 6.0 and 7.0 Server Reference Guides
- Enabling Smart Card Logon for Microsoft Windows Server 2003 and 2008 Reference Guides
- 90Meter Middleware v1.2 Test Report
- Enabling Mozilla Thunderbird for PKI Secured Email
- Wireless Local Area Network (WLAN) Public Key Enablement (PKE) Configuration
- Configuring Squid 2.6 to Cache DoD Certificate Revocation List (CRL) Data.

### New SIPRNet Reference Guides:

- Tumbleweed Desktop Validator 4.10 Workstation Configuration for SIPRNet
- Enabling Smart Card Logon for Microsoft Windows Server 2003 and 2008 Using DoD PKI for SIPR Networks
- Installing & Configuring 90meter SmartCard Manager Middleware
- Configuring 90meter Middleware for Exclusive Acceptance of SIPR- or NIPR-only Tokens
- Enabling Publish to Global Address List (GAL) Feature of 90meter Middleware
- Installing Required DoD and National Security Services (NSS) Certificates in the Trust Store
- Forgotten PIN or Locked SIPRNet Smart Card Procedures
- Sending and Receiving Digitally Signed and Encrypted E-mail Using Outlook 2007

## Upcoming Events

### 2011 Information Assurance Symposium (IAS)

March 7 – 10, 2011

Gaylord Opryland Nashville
2800 Opryland Drive
Nashville, TN 38214

http://www.nsa.gov/ia/events

### 2011 Identity Protection and Management Conference

April 18 – 21, 2011

Renaissance Orlando at SeaWorld
6677 Sea Harbor Drive
Orlando, FL 32821

http://www.nsa.gov/ia/events